CLAIMS

What is claimed is:

1. A method for distributing data over a network comprising:

issuing a certificate and a private key to a client for identifying the client in a transaction;

storing the certificate and the private key in a token used by the client during a transaction;

verifying a digital signature using the certificate stored in the token before distributing data to the client;

generating a message associated with the data being downloaded to the client and associated with the token used by the client during a transaction; and

distributing the data and the associated message to the client.

2. The method of Claim 1, further comprising providing the client with information necessary for establishing an account.

3. The method of Claim 2, further comprising providing the client with the token.

4. A method for distributing data over a network comprising:

establishing a secure connection between a client and a server;

issuing a certificate and a private key to the client for identifying the client in a transaction; and

storing the certificate and the private key in a token used by the client during a transaction.

5. The method of Claim 4, further comprising distributing data to the client.

6. The method of Claim 5, further comprising requesting information from the client for establishing an account.

7. The method of Claim 4, wherein establishing a secure connection comprises establishing a secure connection using a security protocol.

8. The method of Claim 7, wherein the security protocol is the secure socket layer protocol.

9. The method of Claim 6, wherein requesting information comprises requesting a credit card number.

10. The method of Claim 6, wherein requesting information comprises requesting a password.

11. The method of Claim 4, wherein storing the certificate comprises:

interfacing the token to a client computer; and

writing the certificate and the private key to the token across the network.

12. The method of Claim 4, wherein storing the certificate comprises:

interfacing the token to a server computer; and

writing the certificate to the token at the server computer.

13. The method of Claim 5, wherein distributing data to the client comprises distributing a media player.

14. A method for distributing data over a network comprising:

establishing a secure connection between a client and a server;

receiving a request from the client for data to be downloaded;

generating a message associated with the data being downloaded to the client and associated with a token used by the client; and

distributing the data and the associated message to the client.

15. The method of Claim 14, wherein establishing a secure connection comprises establishing a secure connection using a security protocol.

16. The method of Claim 15, wherein the security protocol is the secure socket layer protocol.

17. The method of Claim 14, wherein establishing a secure connection comprises

requesting authentication information from the client; and

sending authentication information from the server.

18. The method of Claim 17, wherein requesting authentication information from the client comprises

requesting a certificate from the client; and

requesting a digital signature from the client.

19. The method of Claim 17, wherein sending authentication information from the server comprises

sending a certificate from the server; and

sending a digital signature from the server.

20. The method of Claim 18, wherein requesting a certificate comprises reading the certificate from the token used by the client.

21. The method of Claim 14, wherein generating a message further comprises:

including in the message a data identification number;

including in the message a period of time for which the data may be used by the client;

including in the message a distinguishing number of the token used by the client when requesting data;

including in the message a symmetrical key used to encrypt the data when distributing data from the server to the client over the network.

22. The method of Claim 14, wherein generating a message further comprises generating a message using a public key (asymmetric) cryptographic algorithm.

23. A method of securely utilizing downloaded data comprising:

opening a media player;

opening a data file;

requesting a token from a client;

reading a distinguishing number from the token;

verifying a digital message associated with the data file and the token using the media player, the distinguishing number, and a private key in the token.

24. The method of Claim 23, wherein in verifying a digital message, the media player reads the private key from the token to decrypt the digital message.

25. The method of Claim 23, wherein in verifying a digital message, the media player sends the digital message to the token.

26. The method of Claim 25, wherein the token decrypts an encrypted symmetric key using the private key.

27. The method of Claim 22, wherein verifying a digital message comprises

verifying the distinguishing number read from the token;

verifying a time period associated with the data file;

decrypting an encrypted symmetrical key using the private key from the token;

decrypting the data file using the symmetrical key.

28. A system for distributing data over a network comprising:

a client computer for requesting data over a network, the client computer being interfaced to the network;

a server computer for distributing requested data over a network, the server computer being interfaced to the network; and

a token interfaced to the client computer,

wherein the server computer stores a certificate and a private key in the token.

29. The system of Claim 28, wherein the server computer verifies an identity of the client with the certificate in the token before distributing data to the client.

30. The system of Claim 28, further comprising

a firewall interfaced to the network; and

a cryptographic processor interfaced to the server computer and the firewall.

31. A system for distributing data over a network comprising:

a client computer for requesting data over a network, the client computer interfaced to the network;

a server computer for distributing requested data over a network, the server computer interfaced to the network;

a token interfaced to the client computer; and

a third party computer system interfaced to the network,

wherein the third party computer system issues a certificate and stores the certificate in the token.

32. The method of Claim 31, wherein the third party computer system issues a private key and stores the private key in the token.